UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/521,833	08/01/2005	Sebastien Canard	072691-017	2404

33401 7590 02/03/2009

MCDERMOTT WILL & EMERY LLP
2049 CENTURY PARK EAST
38th Floor
LOS ANGELES, CA 90067-3208

EXAMINER	
SMITHERS, MATTHEW	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
02/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/521,833	CANARD ET AL.	
	Examiner	Art Unit	
	Matthew B. Smithers	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 6-15* is/are rejected.

7)☒ Claim(s) *4-5* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 6, 7, 12 and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by US 7,028,180 granted to Aull et al.

Regarding claim 1, Aull meets the claimed limitations as follows:

"A list signature method comprising:

an organizing phase including, for a reliable authority defining parameters for implementing an anonymous electronic signature, including a private key and a corresponding public key;

a phase of registering persons in a list of members authorized to generate an electronic signature specific to the members of the list, during which each person to be registered, calculates a private key by means of parameters provided by the reliable authority and by parameters randomly selected by the person to be registered, and the reliable authority delivers to each person to be registered, a certificate of membership of the list;

a phase of defining a sequence including for the reliable authority, generating a serial

number to be used in a signing phase;

a signing phase during which a member of the list generates and issues a signature specific to the members of the list, this signature being built so as to contain proof that the member of the list having issued the signature, has a certificate of membership of the list, and a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the signature;

a phase of verifying the issued signature, comprising steps of applying a predefined algorithm in order to show proof that the signature was issued by a person having a certificate of membership of the list, and verifying using said signature element that the serial number was used for generating the signature;

a phase of revoking a member of the list in order to remove a member from the list, during which the reliable authority removes the member to be removed withdrawn from the list and updates the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the member from the list; and

a phase of updating certificates of the members of the list in order to take into account changes in the composition of the list." see Abstract; column 7, line 24 to column 11, line 32; column 12, lines 25-39 and Figures 1-9.

Regarding claim 2, Aull meets the claimed limitations as follows:

"The method according to claim 1, wherein the organizing phase comprises the definition of a common parameter depending on the composition of the list, the phase for registering a person in the list comprising the definition of a parameter specific to the

person to be registered which is calculated according to the parameter depending on the composition of the list and which is integrated into the certificate out to the person, the registering phase comprising a step of updating the common parameter depending on the composition of the list, the phase of revoking a member of the list comprising a step of changing the common parameter depending on the composition of the list, in order to take into account the removal of the member from the list, and the phase of updating certificates of the members of the list including a step for updating the parameter specific to each member of the list in order to take into account changes in the composition of the list." see Abstract; column 7, line 24 to column 11, line 32; column 12, lines 25-39 and Figures 1-9.

Regarding claim 3, Aull meets the claimed limitations as follows:

"The method according to claim 1 or 2, wherein a signature specific to a member of the list and having the certificate comprises parameters T_1, T_2, T_3, such that: $T_1 = A_i b^w \pmod n$, $T_2 = g^w \pmod n$, $T_3 = g^{e_i} h^w \pmod n$, w being a number randomly selected during the signing phase and b, g, h and n being general parameters for implementing the group signature, such that parameters b, g and h cannot be inferred from each other by integer power raising modulo n functions, so that the number A_i and therefore the identity of the member of the list having the certificate $[A_i, e_i]$ cannot be inferred from a signature issued by the member." see Abstract; column 7, line 24 to column 11, line 32; column 12, lines 25-39 and Figures 1-9.

Regarding claim 6, Aull meets the claimed limitations as follows:

"The method according to claim 1, wherein a signature issued by a member of the list

contains a parameter which is calculated according to the serial number and the private key of the signatory member." see Abstract; column 7, line 24 to column 11, line 32; column 12, lines 25-39 and Figures 1-9.

Regarding claim 7, Aull meets the claimed limitations as follows:

"The method according to claim 6, wherein the parameter T, of a signature issued by a member of the list and depending on the serial number m and on the private key x of the signatory member is obtained by the following formula:

$T4 = m^{x_i} \pmod{n}$

n being a general parameter for implementing the group signature, and the signature comprises proof that the parameter T4 was calculated with the private key xi of the member of the list who issued the signature." see Abstract; column 7, line 24 to column 11, line 32; column 12, lines 25-39 and Figures 1-9.

Regarding claim 12, Aull meets the claimed limitations as follows:

"A server for organizing a list signature comprising means for: generating parameters for implementing an anonymous electronic signature, specific to members of a list, said parameters including a private key and a corresponding public key;

transmitting each person to be registered in said list parameters to be used for calculating a private key by means of parameters randomly selected by the person to be registered, and a certificate of membership of the list;

generating a serial number to be used by the members registered in said list for generating an anonymous signature specific to the members of the list, this signature being built so as to contain a proof that the member of the list having issued the

signature, has a certificate of membership of the list, and a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the signature;

removing a member of the list to be revoked, and updating the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the revoked member from the list; and updating the certificates of the members of the list each time the composition of the list is changed." see Abstract; column 7, line 24 to column 11, line 32; column 12, lines 25-39 and Figures 1-9.

Regarding claim 14, Aull meets the claimed limitations as follows:

"A terminal for generating a list signature comprising means for:

receiving from a reliable authority parameters to be used for calculating a private key;

calculating a private key by means of the received parameters and parameters randomly selected;

receiving from the reliable authority a certificate of membership of the list;

receiving a serial number to be used for generating an anonymous signature specific to the members of the list;

generating an anonymous signature specific to the members of the list, this signature being built so as to contain a proof that the member of the list having issued the signature, has a certificate of membership of the list, and a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the

signature;

verifying a signature issued by a member of said list by applying a predefined algorithm in order to show proof that the signature was issued by a person having a certificate of membership of the list, and by verifying using said signature element that the serial number was used for generating the signature; and

receiving a new certificate of membership of the list each time the composition of the list is changed." see Abstract; column 7, line 24 to column 11, line 32; column 12, lines 25-39 and Figures 1-9.

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 8-11, 13, and 15 are rejected under 35 U.S.C. 102(e) as being anticipated by US 20020077887 granted to London Shrader et al.

Regarding claim 8, London Shrader meets the claimed limitations as follows: "An electronic voting method comprising: an organizing phase of a poll including, for a reliable authority, defining parameters for implementing an anonymous electronic signature for being used to sign a ballot, said parameter including a private key and a

corresponding public key; and of assigning keys to scrutineers, allowing them to decrypt and verify ballots poll;

a phase of registering voters in a list of voters authorized to generate an electronic signature specific to the members of the list, during which each voter to be registered calculates a private key by means of parameters provided by the reliable authority and by parameters randomly selected by the voter to be registered, and the reliable authority delivers to each voter to be registered, a certificate of membership of the list of voter;

a phase of defining a sequence for the elections including, for the reliable authority, generating a serial number to be used in a voting phase;

a voting phase during which the voters of the list of voters sign a ballot by issuing a signature specific to the members of the list of voters, this signature being built so as to contain a proof that the member of the list of voters having issued the signature, has a certificate of membership of the list, and a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the signature; and

a counting phase during which the scrutineers verify the ballots and calculate the result of the poll according to the contents of the decrypted and valid ballots, the verification of a ballot comprising steps of applying a predefined algorithm in order to show proof that the signature was issued by a person having a certificate of membership of the list of voters, and verifying using said signature element that the serial number was used for

generating the signature, in order to detect whether a same voter has issued several ballots for the poll or not;

a phase of revoking a member of the list of voters in order to remove a member from the list, during which the reliable authority removes the member to be removed from the list of voters and updates the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the member from the list; and

a phase of updating certificates of the members of the list of voters in order to take into account changes in the composition of the list." see Abstract; paragraphs [0053]-[0068]; and Figures 1a, 1b and 3-8.

Regarding claim 9, London Shrader meets the claimed limitations as follows: "The voting method according to claim 8, wherein the organizing phase comprises the handing out to each scrutineer of a public key and a private key, the ballots are encrypted by means of a public key obtained by the product of the respective public keys of all the scrutineers, and the corresponding decryption private key is obtained by calculating the sum of the respective private keys of all the scrutineers." see Abstract; paragraphs [0053]-[0068]; and Figures 1a, 1b and 3-8.

Regarding claim 10, London Shrader meets the claimed limitations as follows: "The voting method according to claim 9, wherein encryption of the ballot is carried out by means of a probabilistic encryption algorithm." see Abstract; paragraphs [0053]-[0068]; and Figures 1a, 1b and 3-8.

Regarding claim 11, London Shrader meets the claimed limitations as follows: "The voting method according to claim 8, wherein the ballots issued by the votes are

stored in a public database, in that the result of the verification and counting of each ballot is stored in the database in association with the ballot, and in that the private key for decrypting the ballots is published." see Abstract; paragraphs [0053]-[0068]; and Figures 1a, 1b and 3-8.

Regarding claim 13, London Shrader meets the claimed limitations as follows: "A server for organizing an electronic vote comprising means for: generating during a poll organization phase parameters for implementing an anonymous electronic signature for being used to sign a ballot, said parameter including a private key and a corresponding public key;

generating keys to be assigned to scrutineers, allowing them to decrypt and verify signatures of ballots issued by voters for the poll, said signature being specific to members of a list of voters;

transmitting to each person to be registered in the list of voters parameters to be used for calculating a private key by means of parameters randomly selected by the person to be registered, and a certificate of membership of the list;

generating a serial number specific to the poll, to be used by the members registered in said list of voters for generating an anonymous signature of a ballot specific to the members of the list of voters, this signature of a ballot being built so as to contain a proof that the member of the list of voters having issued the signature, has a certificate of membership of the list of voters, and a signature element which is common to all the signatures issued by a same member of the list of voters with a same serial number and which contains proof that the serial number was used for generating the signature;

removing a member of the list of voters to be revoked, and updating the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the revoked member from the list of voters; and

updating the certificates of the members of the list of voters each time the composition of the list for the poll is changed." see Abstract; paragraphs [0053]-[0068]; and Figures 1a, 1b and 3-8.

Regarding claim 15, London Shrader meets the claimed limitations as follows: "A terminal for issuing an electronic signature of a ballot during an electronic vote, comprising means for:

receiving from a reliable authority parameters to be used for calculating a private key;

calculating a private key by means of the received parameters and parameters randomly selected;

receiving from the reliable authority a certificate of membership of a list of voters;

receiving a serial number to be used for generating an anonymous signature of a ballot for said poll, said signature being specific to the members of the list of voters;

generating an anonymous signature specific to the members of the list of voters, this signature being built so as to contain a proof that the member of the list of voters having issued the signature, has a certificate of membership of the list of voters, and a signature element which is common to all the signatures issued by a same member of the list of voters with a same serial number and which contains proof that the serial number was used for generating the signature;

verifying a signature issued by a member of said list of voters by applying a predefined algorithm in order to show proof that the signature was issued by a person having a certificate of membership of the list of voters, and by verifying using said signature element that the serial number was used for generating the signature; and

receiving a new certificate of membership of the list of voters each time the composition of the list of voters is changed." see Abstract; paragraphs [0053]-[0068]; and Figures 1a, 1b and 3-8.

Allowable Subject Matter

Claims 4 and 5 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 4 and 5, the cited prior art fails to specifically teach the number of the series used for generating a list signature is calculated as a function of a date of the beginning of the series and the function for calculating the number of a series is of the form: $F(d) = (H(d))2 \pmod n$ wherein H is a collision-resistant hash function, d is the date of the beginning of the series, and n is a general parameter for implementing the group signature.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Gentry (US 20080313465) discloses a method for generating signature schemes using bilinear mappings.

B. Kamerman et al (US 20030190046) discloses a system for providing an anonymous signing protocol.

C. McClure et al (US 20030066872) discloses an electronic voting system.

D. Rodriguez et al (US 20020138341) discloses a system for electronic voting over a network.

E. Oishi (US 6,298,153) discloses a method for generating digital signatures in a communication system.

F. Oishi (US 6,154,841) discloses a system for verifying communications whil maintaining anonymity.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew B Smithers/
Primary Examiner, Art Unit 2437